RISK AUDIT

for

Degen

DISTILLERY

on

August 01, 2024

FIDESIUM

Executive Summary

Report

28
/100

TOTAL

Medium risk

August 01, 2024

Abstract

Fidesium's automated risk assessment service was requested to perform a risk posture audit on DegenDistillery's $DRINK token, deployed to Ethereum mainnet at address

```
0x2dc90Fa3a0f178ba4beE16CAc5D6c9A5a7B4C6cB
```

Degen Distillery is an RWA protocol which seeks to tokenize beverage distribution.

Issue Summary

🟥 Critical	🟧 High	🟨 Medium	🟩 Low	◼ Info
0 Issues	0 Issues	1 Issues	4 Issues	1 Issues

Test Approach

Fidesium performed both Whitebox and Blackbox testing, as per the scope of the engagement, and relied on automated security testing.

Caveats

This audit was conducted at block 20434641. Access to the undeployed codebase was not provided, and developer hygiene was not verified. As such test coverage and other development practices have not been included in this assessment.

While the product vision is wildly innovative, the $DRINK token is an ERC-20.

Roughly 0.3% liquidity is held by an upgradeable proxy contract:

```
0x6E17C74C6AF5A6aCb4C68f19DB76d803C1B311dF
```

By analyzing storage slots, an implementation contract was found here:

```
0x4c5dce0a16459a2d39eac8b7c52d3cf82ccdc908
```

This contract is unverified and an ABI has not been provided.

Additional risks where they exist as a function of this being a prelaunch assessment. As such, whale distribution and liquidity risks are not presently included in this rating.

Methodology

The assessment methodology covered a range of phases and employed various tools, including but not limited to the following:

- Mapping Content and Functionality of API
- Application Logic Flaws
- Access Handling
- Authentication/Authorization Flaws
- Brute Force Attempt
- Input Handling
- Source Code Review
- Fuzzing of all input parameter
- Dependency Analysis

Severity Definitions

Critical	The issue can cause large economic losses, large-scale data disorder or loss of control of authority management.
High	The issue puts users' sensitive information at risk or is likely to lead to catastrophic financial implications.
Medium	The issue puts a subset of users' sensitive information at risk, reputation damage or moderate financial impact.
Low	The risk is relatively small and could not be exploited on a recurring basis, or is low-impact to the client's business.
Informational	The issue does not pose an immediate risk but is relevant to security best practices or defence in Depth.

Risk Overview

Team Risk

Low risk: 1

No issues found in founding team

Doxxing Status	Team Experience	Risk Summary
Public	Highly relevant	Low

Whale concentration

Holders

As this is a prelaunch assessment, whale concentration risks have not been asessed. That said, there are currently three holders:

```
1.  0x9F7dc5B7a258F3ABCFBfD288fc63559874C79144
```

```
2.  0x7d36697B9e4e91CA3e1F3081aFAA8DC8fF1A47A9
```

```
3. 0x6E17C74C6AF5A6aCb4C68f19DB76d803C1B311dF
```

Address 1. is holding over 99% of the token. Contract 2. is an unverified contract and an upgradeable proxty with an unverified implementation, holding 0.4% of the liquidity. Contract 3. is an upgradeable transparent proxy, with an implemntation as an unverified contract:

Address 2's implementation is deployed by a known good actor (Kaizen Finance) mitigating the risk.

Liquidity

Risk summary: N/A

As this is a prelaunch assessment, liquidity risks have not been assessed

Whale concentration

Funding

```
0x6E17C74C6AF5A6aCb4C68f19DB76d803C1B311dF
```

Funded by:

```
1. 0x5f9B6C6510BF3c3F2fDFBcB526F5458a08f3fccf
```

```
2. 0xB5359AfCe552240C6EF3c48C321A40EF21DEffaB
```

```
3. 0xB44889a0Da462090922F72D7FaF69bCEB3aDb7C6
```

While proxy contracts and unverified contracts are by ranking "large" holders, the total amount of the token being held by these entities (and therefore the potential impact on the ecosystem) is negligibly low.

Due to the negligible quantities of **$DRINK** stored in these contracts, decompilation was not carried out on the bytecode

While a private wallet holds an overwhelming percentage of the supply, and there is evidence of sybilling, this token is prelaunch, and this is expected.

Vulnerabilities Medium

Reentrancy

Vulnerability severity: **Medium**

Vulnerability probability: **High**

The _transfer function utilizes the following code:

```
if (_statsTracker != address(0)) {
    IStatsTracker(_statsTracker).updateTransferStats(address(this), sender, recipient, amount);
}
```

In principle, if a malicious contract were to be deployed to an address stored at _statsTracker, the external call to >updateTransferStats could be used to recursively call _transfer. This vulnerability then cascades to all callign functions, such as `transferFrom`. This vulnerability is somewhat mitigated by being gated to the statsTracker contract, which can only be set by the contract admin.

Recommendation: Apply the *check-effects-interactions* pattern. In this instance, the full code of the _transfer function shoud be modified to move the `IStatsTracker` call to the end of the function definition. Additionally Fidesium recommends the application of the nonReentrant() guard

Vulnerabilities Low

Missing zero check

Vulnerability severity: **Low**

Vulnerability probability: **Low**

`changeAdmin` does not ensure that a non zero valus is passed on `adminCandidate`. This could allow `adminCandidate` to be set to zero non deliberately.

Missing zero check

Vulnerability severity: **Low**

Vulnerability probability: **Low**

`constructor` does not ensure that a non zero valus is passed on `statsTracker_`. This could allow `statsTracker_` to be set to zero non deliberately.

Missing zero check

Vulnerability severity: **Low**

Vulnerability probability: **Low**

`setStatsTracker` does not ensure that a non zero valus is passed on `statsTracker`. This could allow `statsTracker` to be set to zero non deliberately.

Missing zero check

Vulnerability severity: **Low**

Vulnerability probability: **Low**

`constructor` does not ensure that a non zero valus is passed on `admin_`. This could allow `admin_` to be set to zero non deliberately.

Vulnerabilities Informational

Solc Version

Vulnerability severity: **Info**

Vulnerability probability: **Info**

The contract was deployed with solc 0.8.4. There are no specific known security vulnerabilities in this version, however it is recommended to always use the latest solc to ensure access to all bugfixes and security infrastructure

Missing immutable annotation

Vulnerability severity: **Info**

Vulnerability probability: **Info**

`_decimals` is only set in the constructor, and never modified. It should be marked as `immutable` to save gas.

Disclaimer

Disclaimer

This report is governed by the Fidesium terms and conditions.

This report does not constitute an endorsement or disapproval of any project or team, nor does it reflect the economic value or potential of any related product or asset. It is not investment advice and should not be used as the basis for investment decisions. Instead, this report provides an assessment intended to improve code quality and mitigate risks inherent in cryptographic tokens and blockchain technology.

Fidesium does not guarantee the absence of bugs or vulnerabilities in the technology assessed, nor does it comment on the business practices, models, or regulatory compliance of its creators. All services, reports, and materials are provided "as is" and "as available," without warranties of any kind, including but not limited to merchantability, fitness for a particular purpose, or non-infringement.

Cryptographic assets and blockchain technologies are novel and carry inherent technical risks, uncertainties, and the possibility of unpredictable outcomes. Assessment results may contain inaccuracies or depend on third-party systems, and reliance on them is solely at the Customer’s risk.

Fidesium assumes no liability for content inaccuracies, personal injuries, property damages, or losses related to the use of its services, reports, or materials. Third-party components are provided "as is," and any warranties are strictly between the Customer and the third-party provider.

These services and materials are intended solely for the Customer's use and benefit. No third party or their representatives may claim rights to or rely on these services, reports, or materials under any circumstances.